

# A quadratically tight partition bound for classical communication complexity and query complexity

Rahul Jain\*   Troy Lee†   Nisheeth K. Vishnoi‡

## Abstract

In this work we introduce, both for classical communication complexity and query complexity, a modification of the *partition bound* introduced by Jain and Klauck [JK10]. We call it the *public-coin partition bound*. We show that (the logarithm to the base two of) its communication complexity and query complexity versions form, for all relations, a quadratically tight lower bound on the public-coin randomized communication complexity and randomized query complexity respectively.

**Keywords:** Partition bound, communication complexity, lower bounds, linear programs.

## 1 Introduction

The *partition bound* introduced by Jain and Klauck [JK10] is known to be one of the strongest lower bound methods in classical communication complexity and query complexity. It is known to be stronger than most other lower bound methods, both in communication complexity and query complexity, except its relationship with the *information complexity* lower bound method in communication complexity is unknown. It is an interesting open question, in both these settings, as to how tight this lower bound method is. We are not aware, to the best of our knowledge, of any function or relation where this method is asymptotically weaker either for communication complexity or for query complexity.

In this work we introduce, both for communication complexity and query complexity, a modification of the partition bound which we call the *public-coin partition bound*. Analogous to the partition bound, our new bound is also a linear-programming based lower bound method. We show that (the logarithm to the base two of) its communication and query complexity versions continue to form a lower bound on the public-coin communication complexity and randomized query complexity respectively. In addition we show that the square of (the logarithm to the base two of) its communication and query complexity versions form an upper bound on the public-coin communication complexity and randomized query complexity respectively. Also it is easily seen via their linear programs that our new bound is stronger than the partition bound for all relations, both in communication complexity and query complexity.

---

\*Centre for Quantum Technologies and Department of Computer Science, National University of Singapore. Email: rahul@comp.nus.edu.sg

†Nanyang Technological University and Center for Quantum Technologies. Email: troyjlee@gmail.com

‡Microsoft Research, India. Email: nisheeth.vishnoi@gmail.com

## 2 Communication complexity

In this section we introduce our new bound in the communication complexity setting. Let us first recall the partition bound of [JK10].

**Definition 1 (Partition bound [JK10])** *Let  $f \subseteq \mathcal{X} \times \mathcal{Y} \times \mathcal{Z}$  be a relation. Let  $\epsilon > 0$ . The  $\epsilon$ -partition bound of  $f$ , denoted  $\text{prt}_\epsilon(f)$ , is given by the optimal value of the following linear program. Below  $R$  represents a rectangle in  $\mathcal{X} \times \mathcal{Y}$  and  $(x, y, z) \in \mathcal{X} \times \mathcal{Y} \times \mathcal{Z}$ .*

$$\begin{array}{ll}
 \text{Primal} & \text{Dual} \\
 \min: & \sum_z \sum_R w_{z,R} \\
 \forall(x, y): & \sum_{z:(x,y,z) \in f} \sum_{R:(x,y) \in R} w_{z,R} \geq 1 - \epsilon, \\
 \forall(x, y): & \sum_{R:(x,y) \in R} \sum_z w_{z,R} = 1, \\
 \forall(z, R): & w_{z,R} \geq 0. \\
 \end{array}
 \qquad
 \begin{array}{ll}
 \max: & (1 - \epsilon) \sum_{(x,y)} \mu_{x,y} + \sum_{(x,y)} \phi_{x,y} \\
 \forall(z, R): & \sum_{(x,y) \in R:(x,y,z) \in f} \mu_{x,y} + \sum_{(x,y) \in R} \phi_{x,y} \leq 1, \\
 \forall(x, y): & \mu_{x,y} \geq 0, \phi_{x,y} \in \mathbb{R}.
 \end{array}$$

Our new bound is defined as follows.

**Definition 2 (Public-coin partition bound)** *Let  $f \subseteq \mathcal{X} \times \mathcal{Y} \times \mathcal{Z}$  be a relation. Let  $\epsilon > 0$ . The  $\epsilon$ -public-coin partition bound of  $f$ , denoted  $\text{pprt}_\epsilon(f)$ , is given by the optimal value of the following linear program. Below  $R$  represents a rectangle in  $\mathcal{X} \times \mathcal{Y}$  and  $P$  represents a partition along with outputs in  $\mathcal{Z}$ ; that is  $P = \{(z_1, R_1), (z_2, R_2), \dots, (z_m, R_m)\}$ , such that  $\{R_1, \dots, R_m\}$  form a partition of  $\mathcal{X} \times \mathcal{Y}$  into rectangles and  $\forall i \in [m], z_i \in \mathcal{Z}$ .*

$$\begin{array}{ll}
 \text{Primal} & \text{Dual} \\
 \min: & \sum_z \sum_R w_{z,R} \\
 \forall(x, y): & \sum_{z:(x,y,z) \in f} \sum_{R:(x,y) \in R} w_{z,R} \geq 1 - \epsilon, \\
 \forall(x, y): & \sum_{R:(x,y) \in R} \sum_z w_{z,R} = 1, \\
 \forall(z, R): & w_{z,R} = \sum_{P:(z,R) \in P} a_P, \\
 \sum_P a_P & = 1, \\
 \forall(z, R): & w_{z,R} \geq 0; \quad \forall P: a_P \geq 0. \\
 \end{array}
 \qquad
 \begin{array}{ll}
 \max: & (1 - \epsilon) \sum_{(x,y)} \mu_{x,y} + \sum_{(x,y)} \phi_{x,y} + \lambda \\
 \forall(z, R): & \sum_{(x,y) \in R:(x,y,z) \in f} \mu_{x,y} + \sum_{(x,y) \in R} \phi_{x,y} + v_{z,R} \leq 1, \\
 \forall P: & \sum_{(z,R) \in P} v_{z,R} \geq \lambda, \\
 \forall(x, y): & \mu_{x,y} \geq 0, \phi_{x,y} \in \mathbb{R}; \quad \forall(z, R): v_{z,R} \in \mathbb{R}, \\
 \lambda & \in \mathbb{R}.
 \end{array}$$

We show that (the logarithm to the base two of) it is a lower bound on public-coin randomized communication complexity (please refer to [KN97] for standard definitions in communication complexity).

**Lemma 1** *Let  $f \subseteq \mathcal{X} \times \mathcal{Y} \times \mathcal{Z}$  be a relation. Let  $\epsilon > 0$ . Let  $R_\epsilon^{\text{pub}}(f)$  represents the public-coin communication complexity of  $f$  with worst-case error  $\epsilon$ . Then,*

$$\log_2 \text{pprt}_\epsilon(f) \leq R_\epsilon^{\text{pub}}(f).$$

**Proof** This proof goes along similar lines as the proof of [JK10] for analogous result about the partition bound.

Let  $\mathcal{P}$  be a public coin randomized protocol for  $f$  with communication  $c \stackrel{\text{def}}{=} R_\epsilon^{\text{pub}}(f)$  and worst case error  $\epsilon$ . For binary string  $r$ , let  $\mathcal{P}_r$  represent the deterministic communication protocol obtained from  $\mathcal{P}$  on fixing the public coins to  $r$ . Every deterministic communication protocol amounts to partitioning the inputs in  $\mathcal{X} \times \mathcal{Y}$  into rectangles and outputting an element in  $\mathcal{Z}$  corresponding to each rectangle in the partition. Let  $P_r = \{(z_1^r, R_1^r), (z_2^r, R_2^r), \dots, (z_m^r, R_m^r)\}$ , be the corresponding partition along with the outputs, that is  $\{R_1^r, \dots, R_m^r\}$  form a partition of  $\mathcal{X} \times \mathcal{Y}$  into rectangles and  $\forall i \in [m], z_i^r \in \mathcal{Z}$ . Let  $q_r$  represent the probability of string  $r$  in  $\mathcal{P}$ . For  $P_r$  define  $a'_{P_r} \stackrel{\text{def}}{=} q_r$ . For the partitions  $P$  that do not correspond to any random string  $r$  in  $\mathcal{P}$ , define  $a'_P = 0$ . For any  $(z, R)$  define,

$$w'_{z,R} \stackrel{\text{def}}{=} \sum_{P:(z,R) \in P} a'_P .$$

It is easily seen that for all  $(x, y, z) \in \mathcal{X} \times \mathcal{Y} \times \mathcal{Z}$ :

$$\Pr[\mathcal{P} \text{ outputs } z \text{ on input } (x, y)] = \sum_{R:(x,y) \in R} w'_{z,R} .$$

Since the protocol has error at most  $\epsilon$  on all inputs we get the constraints:

$$\forall (x, y) : \sum_{z:(x,y,z) \in f} \sum_{R:(x,y) \in R} w'_{z,R} \geq 1 - \epsilon .$$

Also since the  $\Pr[\mathcal{P} \text{ outputs some } z \in \mathcal{Z} \text{ on input } (x, y)] = 1$ , we get the constraints:

$$\forall (x, y) : \sum_z \sum_{R:(x,y) \in R} w'_{z,R} = 1 .$$

We also have by construction:

$$\sum_P a'_P = 1; \quad \forall (z, R) : w'_{z,R} \geq 0; \quad \forall P : a'_P \geq 0 .$$

Therefore  $\{w'_{z,R}\} \cup \{a'_P\}$  is feasible for the primal of  $\text{pprt}_\epsilon(f)$ .

We know that for each  $r$ ,  $|P_r| \leq 2^c$ , since the communication in  $\mathcal{P}_r$  is at most  $c$  bits. Hence,

$$\text{pprt}_\epsilon(f) \leq \sum_z \sum_R w'_{z,R} = \sum_r a'_{P_r} \cdot |P_r| \leq 2^c \sum_r a'_{P_r} = 2^c .$$

□

Next we show that the square of (the logarithm to the base two of) our new bound forms an upper bound on the public-coin communication complexity.

**Theorem 1** *Let  $f \subseteq \mathcal{X} \times \mathcal{Y} \times \mathcal{Z}$  be a relation. Let  $\epsilon > 0$ . We have,*

$$R_{2\epsilon}^{\text{pub}}(f) \leq \left( \log_2 \text{pprt}_\epsilon(f) + \log_2 \frac{1}{\epsilon} + 1 \right)^2 .$$

**Proof** Let  $\text{pprt}_\epsilon(f) = 2^c$ . Let  $\{w_{z,R}\} \cup \{a_P\}$  be an optimal solution for the primal. Let  $n_P$  be the number of rectangles in  $P$ . We have,

$$\sum_P a_P \cdot n_P = \sum_{z,R} w_{z,R} = 2^c.$$

Define  $B \stackrel{\text{def}}{=} \{P \mid n_P \geq \frac{1}{\epsilon} 2^c\}$ . Then  $\delta \stackrel{\text{def}}{=} \sum_{P \in B} a_P \leq \epsilon$ . Define  $a'_P \stackrel{\text{def}}{=} \frac{1}{1-\delta} a_P$  for  $P \notin B$  and  $a'_P \stackrel{\text{def}}{=} 0$  for  $P \in B$ . Define  $w'_{z,R} \stackrel{\text{def}}{=} \sum_{P:(z,R) \in P} a'_P$ . Then we have,

$$\begin{aligned} \forall(x, y) : \quad & \sum_{z:(x,y,z) \in f} \sum_{R:(x,y) \in R} w'_{z,R} \geq 1 - 2\epsilon, \\ \forall(x, y) : \quad & \sum_{R:(x,y) \in R} \sum_z w'_{z,R} = 1, \\ \forall(z, R) : \quad & w'_{z,R} = \sum_{P:(z,R) \in P} a'_P, \\ & \sum_P a'_P = 1, \\ & \forall(z, R) : w'_{z,R} \geq 0; \quad \forall P : a'_P \geq 0. \end{aligned}$$

We know that a partition with  $m$  rectangles can be realized by a communication protocol with communication  $(\lceil \log_2 m \rceil)^2$  (arguments as in the proof of Theorem 2.11 of [KN97], we reproduce them in Section A for completeness). Consider a public-coin communication protocol  $\Pi$  as follows.

1. Alice and Bob (using public coins) choose a  $P = \{(z_1, R_1), (z_2, R_2), \dots, (z_m, R_m)\}$  with probability  $a'_P$ .
2. They communicate to realize the partition  $\{R_1, R_2, \dots, R_m\}$  with communication bounded by  $(c + \log_2 \frac{1}{\epsilon} + 1)^2$ .
3. If they end up with rectangle  $R_i$ , they output  $z_i$ .

It is clear that the worst case communication of the protocol is bounded by  $(c + \log_2 \frac{1}{\epsilon} + 1)^2$ . The condition,

$$\forall(x, y) : \quad \sum_{z:(x,y,z) \in f} \sum_{R:(x,y) \in R} w'_{z,R} \geq 1 - 2\epsilon,$$

implies that the protocol has worst case error at most  $2\epsilon$ . Therefore,

$$R_{2\epsilon}^{\text{pub}}(f) \leq \left( \log_2 \text{pprt}_\epsilon(f) + \log_2 \frac{1}{\epsilon} + 1 \right)^2.$$

□

### 3 Query complexity

In this section we introduce our new bound in the query complexity setting.

Let  $f \subseteq \{0,1\}^n \times \mathcal{Z}$  be a relation. An *assignment*  $A : S \rightarrow \{0,1\}^l$  is an assignment of values to some subset  $S$  of  $n$  variables (with  $|S| = l$ ). We say that  $A$  is *consistent* with  $x \in \{0,1\}^n$  if  $x_i = A(i)$  for all  $i \in S$ . We write  $x \in A$  as shorthand for ‘ $A$  is consistent with  $x$ ’. We write  $|A|$  to represent the size of  $A$  which is the cardinality of  $S$  (not to be confused with the number of consistent inputs). Furthermore we say that an index  $i$  *appears* in  $A$ , iff  $i \in S$  where  $S$  is the subset of  $[n]$  corresponding to  $A$ . Let  $\mathcal{A}$  denote the set of all assignments. Below we assume  $x \in \{0,1\}^n$ ,  $A \in \mathcal{A}$  and  $z \in \mathcal{Z}$ . Below  $P$  represents a partition along with outputs in  $\mathcal{Z}$ ; that is  $P = \{(z_1, A_1), (z_2, A_2), \dots, (z_m, A_m)\}$ , such that  $\{A_1, \dots, A_m\}$  form a partition of  $\{0,1\}^n$  into assignments (that is for each  $x \in \{0,1\}^n$ , there is a unique  $i \in [m]$  such that  $x \in A_i$ ) and  $\forall i \in [m], z_i \in \mathcal{Z}$ .

Let us first recall the partition bound of [JK10].

**Definition 3 (Partition bound [JK10])** *Let  $f \subseteq \{0,1\}^n \times \mathcal{Z}$  be a relation. Let  $\epsilon > 0$ . The  $\epsilon$ -partition bound of  $f$ , denoted  $\text{prt}_\epsilon(f)$ , is given by the optimal value of the following linear program.*

<u>Primal</u>	<u>Dual</u>
$\min: \sum_z \sum_A w_{z,A} \cdot 2^{ A }$ $\forall x: \sum_{z:(x,z) \in f} \sum_{A:x \in A} w_{z,A} \geq 1 - \epsilon,$ $\forall x: \sum_{A:x \in A} \sum_z w_{z,A} = 1,$ $\forall (z, A): w_{z,A} \geq 0.$	$\max: (1 - \epsilon) \sum_x \mu_x + \sum_x \phi_x$ $\forall (z, A): \sum_{x \in A: (x,z) \in f} \mu_x + \sum_{x \in A} \phi_x \leq 2^{ A },$ $\forall x: \mu_x \geq 0, \phi_x \in \mathbb{R}.$

Our new bound is defined as follows.

**Definition 4 (Public-coin partition bound)** *Let  $f \subseteq \{0,1\}^n \times \mathcal{Z}$  be a relation. Let  $\epsilon > 0$ . The  $\epsilon$ -public-coin partition bound of  $f$ , denoted  $\text{pprt}_\epsilon(f)$ , is given by the optimal value of the following linear program.*

<u>Primal</u>	<u>Dual</u>
$\min: \sum_z \sum_A w_{z,A} \cdot 2^{ A }$ $\forall x: \sum_{z:(x,z) \in f} \sum_{A:x \in A} w_{z,A} \geq 1 - \epsilon,$ $\forall x: \sum_{A:x \in A} \sum_z w_{z,A} = 1,$ $\forall (z, A): w_{z,A} = \sum_{P:(z,A) \in P} a_P,$ $\sum_P a_P = 1,$ $\forall (z, A): w_{z,A} \geq 0; \quad \forall P: a_P \geq 0.$	$\max: (1 - \epsilon) \sum_x \mu_x + \sum_x \phi_x + \lambda$ $\forall (z, A): \sum_{x \in A: (x,z) \in f} \mu_x + \sum_{x \in A} \phi_x + v_{z,A} \leq 2^{ A },$ $\forall P: \sum_{(z,A) \in P} v_{z,A} \geq \lambda,$ $\forall x: \mu_x \geq 0, \phi_x \in \mathbb{R}; \quad \forall (z, A): v_{z,A} \in \mathbb{R},$ $\lambda \in \mathbb{R}.$

We show that (the logarithm to the base two of) our new bound is a lower bound on randomized query complexity.

**Lemma 2** *Let  $f \subseteq \{0, 1\}^n \times \mathcal{Z}$  be a relation. Let  $\epsilon > 0$ . Let  $R_\epsilon(f)$  represent the randomized query complexity of  $f$  with worst case error  $\epsilon$ . Then,*

$$\frac{1}{2} \log_2 \text{pprt}_\epsilon(f) \leq R_\epsilon(f).$$

**Proof** Our proof goes along arguments similar to [JK10] for analogous result for the partition bound.

Let  $\mathcal{P}$  be a randomized query algorithm which achieves  $c \stackrel{\text{def}}{=} R_\epsilon(f)$ . Let  $\mathcal{P}_r$  be the deterministic query algorithm, arising from  $\mathcal{P}$ , corresponding to random string  $r$ . We know that each such deterministic query algorithm is a binary decision tree of depth at most  $c$  (please refer to [BW02] for standard definitions related to query complexity). We note that the roots of a decision tree (together) represent a partition of the inputs into assignments along with outputs in  $\mathcal{Z}$ . Let  $P_r = \{(z_1^r, A_1^r), (z_2^r, A_2^r), \dots, (z_m^r, A_m^r)\}$ , represent the partition along with outputs corresponding to random string  $r$ , where  $\{A_1^r, \dots, A_m^r\}$  form a partition of  $\{0, 1\}^n$  into assignments and  $\forall i \in [m], z_i^r \in \mathcal{Z}$ . Let  $q_r$  represent the probability of string  $r$  in  $\mathcal{P}$ . For  $P_r$  define  $a'_{P_r} \stackrel{\text{def}}{=} q_r$ . For the partitions  $P$  that do not correspond to any string  $r$  in  $\mathcal{P}$ , define  $a'_P = 0$ . For any  $(z, A)$  define,

$$w'_{z,A} \stackrel{\text{def}}{=} \sum_{P:(z,A) \in P} a'_P.$$

As in the proof of Lemma 1, we can argue that  $\{w'_{z,A}\} \cup \{a'_P\}$  is feasible for the primal of  $\text{pprt}_\epsilon(f)$ . Note that for each  $(z, A)$  with  $w'_{z,A} > 0$ , we have  $|A| \leq c$ . Also  $|P_r| \leq 2^c$  since the depth of the corresponding binary decision tree is at most  $c$ . Now,

$$\begin{aligned} \text{pprt}_\epsilon(f) &= \sum_z \sum_A w'_{z,A} 2^{|A|} \leq 2^c \left( \sum_z \sum_A w'_{z,A} \right) \\ &\leq 2^c \left( \sum_r a'_{P_r} \cdot |P_r| \right) \leq 2^{2c} \sum_r a'_{P_r} = 2^{2c}. \end{aligned}$$

Hence our result.  $\square$

Next we show that the square of (the logarithm to the base two of) our new bound forms an upper bound on randomized query complexity.

**Theorem 2** *Let  $f \subseteq \{0, 1\}^n \times \mathcal{Z}$  be a relation. Let  $\epsilon > 0$ . Then,*

$$R_{2\epsilon}(f) \leq \left( \log \text{pprt}_\epsilon(f) + \log_2 \frac{1}{\epsilon} \right)^2.$$

**Proof** Let  $\text{pprt}_\epsilon(f) = 2^c$ . Let  $\{w_{z,A}\} \cup \{a_P\}$  be an optimal solution for the primal. We have,

$$\sum_P \sum_{A:(z,A) \in P} a_P \cdot 2^{|A|} = \sum_{z,A} w_{z,A} \cdot 2^{|A|} = 2^c.$$

Define  $B \stackrel{\text{def}}{=} \{P \mid \exists (z, A) \in P \text{ with } |A| > c + \log_2 \frac{1}{\epsilon}\}$ . Then  $\delta \stackrel{\text{def}}{=} \sum_{P \in B} a_P \leq \epsilon$ . Define  $a'_P \stackrel{\text{def}}{=} \frac{1}{1-\delta} a_P$  for  $P \notin B$  and  $a'_P \stackrel{\text{def}}{=} 0$  for  $P \in B$ . Define  $w'_{z,A} \stackrel{\text{def}}{=} \sum_{P: (z,A) \in P} a'_P$ . Then we have,

$$\begin{aligned} \forall x : \sum_{z: (x,z) \in f} \sum_{A: x \in A} w'_{z,A} &\geq 1 - 2\epsilon, \\ \forall x : \sum_{A: x \in A} \sum_z w'_{z,A} &= 1, \\ \forall (z, A) : w'_{z,A} &= \sum_{P: (z,A) \in P} a'_P, \\ \sum_P a'_P &= 1, \\ \forall (z, A) : w'_{z,A} &\geq 0; \quad \forall P : a'_P \geq 0. \end{aligned}$$

We know that a partition with assignments each of length at most  $m$  can be realized by a query protocol with  $m^2$  queries (arguments as in the proof of Theorem 11 of [BW02], we reproduce them in Section B for completeness). Consider a randomized query protocol  $\Pi$  as follows.

1. Alice (randomly) chooses a  $P = \{(z_1, A_1), (z_2, A_2), \dots, (z_s, A_s)\}$  with probability  $a'_P$ .
2. She queries to realize the partition  $\{A_1, A_2, \dots, A_s\}$  with  $(c + \log_2 \frac{1}{\epsilon})^2$  queries.
3. If she ends up with assignment  $A_i$ , she outputs  $z_i$ .

It is clear that the worst case queries of the protocol is  $(c + \log_2 \frac{1}{\epsilon})^2$ . The condition,

$$\forall x : \sum_{z: (x,z) \in f} \sum_{A: x \in A} w'_{z,A} \geq 1 - 2\epsilon,$$

implies that the protocol has worst case error at most  $2\epsilon$ . Therefore,

$$R_{2\epsilon}(f) \leq \left( \log_2 \text{pprt}_\epsilon(f) + \log_2 \frac{1}{\epsilon} \right)^2.$$

□

## Acknowledgment

The work done is supported by the internal grants of the Center for Quantum Technologies (CQT), Singapore. Part of the work done when N.K.V was visiting CQT.

## References

- [BW02] H. Buhrman and R. de Wolf. Complexity measures and decision tree complexity: A survey. *Theoretical Computer Science*, 288(1):21–43, 2002.
- [JK10] Rahul Jain, Hartmut Klauck. The partition bound for classical communication complexity and query complexity. In *Proceeding of the 25th IEEE Conference on Computational Complexity*, (CCC), pp.247-258, 2010.

- [KN97] E. Kushilevitz and N. Nisan. *Communication Complexity*. Cambridge University Press, 1997.

## A Communication protocol to realize a partition

Let  $\{R_1, R_2, \dots, R_m\}$  be a partition of  $\mathcal{X} \times \mathcal{Y}$ . Let  $x$  and  $y$  be the inputs to Alice and Bob respectively.

1. Alice determines if there exists an  $i \in [m]$  such that the row corresponding to  $x$  intersects with  $R_i$  and the number of rectangles in  $\{R_1, R_2, \dots, R_m\}$  that row intersect with  $R_i$  are at most  $m/2$ . If such  $i$  exists she communicates it to Bob using  $\lceil \log_2 m \rceil$  bits. They both now consider  $\{R_1 \cap R_i, R_2 \cap R_i, \dots, R_m \cap R_i\}$  as a partition of  $(\mathcal{X} \times \mathcal{Y}) \cap R_i$  and repeat. If Alice cannot find any such  $i$  she indicates this to Bob by sending 0.
2. On receiving 0 from Alice, Bob determines if there exists a  $j \in [m]$  such that the column corresponding to  $y$  intersects with  $R_j$  and the number of rectangles in  $\{R_1, R_2, \dots, R_m\}$  that column intersect with  $R_j$  are at most  $m/2$ . If such  $j$  exists he communicates it to Alice using  $\lceil \log_2 m \rceil$  bits. They both now consider  $\{R_1 \cap R_j, R_2 \cap R_j, \dots, R_m \cap R_j\}$  as a partition of  $(\mathcal{X} \times \mathcal{Y}) \cap R_j$  and repeat.

We can note that either Alice or Bob must succeed in finding desired  $i, j$  respectively since the rectangle that contains  $(x, y)$  satisfies the requirements in either 1. or 2. above (since  $\{R_1, R_2, \dots, R_m\}$  is a partition of  $\mathcal{X} \times \mathcal{Y}$ ). Also the communication in each round is at most  $\lceil \log_2 m \rceil$  and the number of (non-empty) rectangles surviving after each round reduce by a factor of 2. Hence the process ends after at most  $\lceil \log_2 m \rceil$  rounds. The total communication hence is bounded by  $(\lceil \log_2 m \rceil)^2$ .

## B Query protocol to realize a partition

Let  $\{A_1, A_2, \dots, A_s\}$  be a partition of  $\{0, 1\}^n$  such that  $|A_i| \leq m$  for each  $i \in [s]$ . Let  $x$  be the string in the database.

1. Alice queries the bits of  $x$  corresponding to  $A_1$ . If the bits revealed are consistent with  $A_1$  then she considers  $A_1$  as desired assignment and stops.
2. If the bits revealed are not consistent with  $A_1$  then we note that one bit is revealed for  $A_i$  for all  $i \in [s]$  (since  $\{A_1, A_2, \dots, A_s\}$  is a partition of  $\{0, 1\}^n$ ). Hence the size of each  $A_i$  (consistent with the bits revealed so far) reduces by at least 1. Alice considers now the new set of (modified)  $A_i$ s which are consistent with the bits revealed so far and repeats.

We note that the number of such rounds is at most  $m$  and in each round at most  $m$  bits are revealed. Hence the total number of queries is at most  $m^2$ .